WE CLAIM:

1. A computer program product comprising a computer program operable to control a computer to detect a malicious alteration to a stored computer file, said computer program comprising:

file comparing logic operable to compare said stored computer file with an archive copy of said computer file stored when said stored computer file was created; and

comparison response logic operable if said file comparing logic detects that said stored computer file and said archive computer file do not match to trigger further countermeasures against a potential malicious alteration.

2. A computer program product as claimed in claim 1, wherein said further countermeasures include scanning said stored computer file using a library of computer virus definition data to identify a computer virus infection of said stored computer file.

3. A computer program product as claimed in claim 1, wherein said archive copy of said computer file is stored in one of:

an unencrypted form;

an encrypted form;

an encrypted media;

an encrypted volume; and

a PGP disk.

4. A computer program product as claimed in claim 1, wherein said archive copy of said computer file is stored in one of:

a different physical storage device to said stored computer file; and

a different part of a common physical storage device shared with stored computer file.

5. A computer program product as claimed in claim 1, wherein a subset of file types stored by said computer are subject comparison by said file comparing logic and to creation of an archive copy for use with said file comparing logic.

6. A computer program product as claimed in claim 5, wherein said subset of file types include one or more of:

executable file types; and

dynamic link library file types.

7. A computer program product as claimed in claim 1, comprising archive file copy logic operable upon creation of said stored computer file to also created said archive copy of said computer file.

8. A computer program product as claimed in claim 7, wherein said archive file copy logic operates to create said archive copy of said computer file for a subset of file types stored by said computer.

9. A computer program product as claimed in claim 8, wherein said subset of file types include one or more of:

executable file types; and

dynamic link library file types.

10. A method of detecting a malicious alteration to a stored computer file, said method comprising the steps of:

comparing said stored computer file with an archive copy of said computer file stored when said stored computer file was created; and

if said file comparing step detects that said stored computer file and said archive computer file do not match, triggering further countermeasures against a potential malicious alteration.

11. A method as claimed in claim 10, wherein said further countermeasures include scanning said stored computer file using a library of computer virus definition data to identify a computer virus infection of said stored computer file.

12. A method as claimed in claim 10, wherein said archive copy of said computer file is stored in one of:

an unencrypted form;

an encrypted form;

an encrypted media;

an encrypted volume; and

a PGP disk.

13. A method as claimed in claim 10, wherein said archive copy of said computer file is stored in one of:

a different physical storage device to said stored computer file; and

a different part of a common physical storage device shared with stored computer file.

14. A method as claimed in claim 10, wherein a subset of file types stored by said computer are subject comparison by said file comparing logic and to creation of an archive copy for use in said comparing step.

15. A method as claimed in claim 14, wherein said subset of file types include one or more of:

executable file types; and

dynamic link library file types.

16. A method as claimed in claim 10, comprising the step of upon creation of said stored computer file also creating said archive copy of said computer file.

17. A method as claimed in claim 16, wherein said step of creating said archive copy operates to create said archive copy of said computer file for a subset of file types stored by said computer.

18. A method as claimed in claim 17, wherein said subset of file types include one or more of:

executable file types; and

dynamic link library file types.

19. Apparatus for processing data operable to detect a malicious alteration to a stored computer file, said apparatus comprising:

a file comparitor operable to compare said stored computer file with an archive copy of said computer file stored when said stored computer file was created; and

a comparison responder operable if said file comparing logic detects that said stored computer file and said archive computer file do not match to trigger further countermeasures against a potential malicious alteration.

20. Apparatus as claimed in claim 19, wherein said further countermeasures include scanning said stored computer file using a library of computer virus definition data to identify a computer virus infection of said stored computer file.

21. Apparatus as claimed in claim 19, wherein said archive copy of said computer file is stored in one of:

an unencrypted form;

an encrypted form;

an encrypted media;

an encrypted volume; and

a PGP disk.

22. Apparatus as claimed in claim 19, wherein said archive copy of said computer file is stored in one of:

a different physical storage device to said stored computer file; and

a different part of a common physical storage device shared with stored computer file.

23. Apparatus as claimed in claim 19, wherein a subset of file types stored by said computer are subject comparison by said file comparitor and to creation of an archive copy for use with said file comparitor.

24. Apparatus as claimed in claim 23, wherein said subset of file types include one or more of:

executable file types; and

dynamic link library file types.

25. Apparatus as claimed in claim 19, comprising an archive file copier operable upon creation of said stored computer file to also created said archive copy of said computer file.

26. Apparatus as claimed in claim 25, wherein said archive file copier operates to create said archive copy of said computer file for a subset of file types stored by said computer.

27. Apparatus as claimed in claim 26, wherein said subset of file types include one or more of:

executable file types; and

dynamic link library file types.